

This listing of claims is provided for the Examiner's convenience.

Listing of Claims:

1. (Original) A computer-implemented method for systematically identifying and characterizing vulnerabilities in a computer system comprising the steps of:

describing a set of potential attacks on the computer system through which a  
5 change in status of the computer system could be effected, wherein the  
change comprises a transition from a start condition to an end condition  
which is different from the start condition;

defining a set of paths comprising at least one path for each potential attack  
described, wherein each path comprises at least one event necessary for  
10 transition from the start condition to the end condition, which transition  
can include passage through intermediate conditions in transit from the  
start condition to the end condition;

for each path in said set of paths, assigning a length value,  $L$ , corresponding to a  
metric reflecting at least one security significant condition bearing on  
15 likelihood of success of an attacker attempting to effect said transition  
from the start condition, through intermediate conditions, if any, to the end  
condition, so that the value of  $L$  correlates inversely with said likelihood of  
success;

identifying within said set of paths at least one shortest path defined as that  
20 having the smallest length value of paths in the set of paths;

identifying, from within the set of paths, specific paths (denoted "epsilon optimal  
paths") having a length,  $L \leq (1+\epsilon)$  times the length of the shortest path,  
where  $\epsilon$  is a non-negative number that accounts for uncertainty in

individual edge metrics and uncertainty in the actual path the attacker will  
25 choose; and

designating “epsilon optimal paths” as high risk attack paths.

2. (Original) The method of claim 1 wherein the at least one security significant condition is selected from the group consisting of

estimated time necessary for the attacker to achieve said success,

estimated cost to the attacker in order to achieve said success,

5 estimated degree of effort by the attacker in order to achieve said success,

estimated likelihood of detection of the attacker’s efforts in attempting to achieve said success,

estimated likelihood of approbation of an attack, and

any combination thereof.

3. (Original) The method of claim 2 further comprising the step of generating a graphical depiction of at least a portion of the set of paths, wherein, for each path, nodes represent discrete physical states of the computer system and edges adjoining nodes represent transitions between physical states in the computer system.

4. (Original) The method of claim 3 wherein nodes shown in the graphical depiction include  
a physical state associated with the start condition,  
a physical state associated with the end condition, and  
physical states associated with intermediate conditions, if any exist for a given path.

5. (Original) The method of claim 4 wherein redundant paths to nodes are eliminated, by enforcing an ordering on acquisition of multiple, independent vulnerabilities in the graph.

6. (Original) The method of claim 5 wherein transitions between physical states in the computer system are characterized mathematically by assigning each transition an edge weight based on at least one security significant metric having an assigned value.

7. (Original) The method of claim 6 wherein the assigned value of the at least one security significant metric is calculated as a function of an element capable of affecting security of the computer system, wherein the element is selected from the group consisting of capabilities of at least one hypothesized attacker and,  
5 network configuration information.

8. (Original) The method of claim 7 wherein the capabilities of the at least one hypothesized attacker are assigned a quantitative value based on a factor selected from the group consisting of:

hypothesized probability of success of the attacker in effecting a given transition  
5 between physical states;

hypothesized cost to the attacker in effecting a given transition between physical  
states;

hypothesized level of effort of the attacker in effecting a given transition between  
physical states

10 hypothesized length of time necessary for the attacker to succeed in effecting a  
given transition between physical states; and  
any combination thereof.

9. (Original) The method of claim 8 further comprising the steps of  
providing at least one configuration file from which is obtained the information  
about the network and machine configuration of the computer system;  
providing at least one attack template comprising hypothesized attack  
5 information which, in turn, comprises at least one attack step which, if  
successful, could effect a change in status of the computer system given  
its configuration; and

providing at least one attacker profile comprising hypothesized attacker

information which, in turn, comprises at least one capability of at least one

10 hypothesized attacker, which, if exercised, could enable said at least one  
attack step to take place successfully.

10. (Original) The method of claim 9 wherein the configuration file is generated as a result of gathering information about the network configuration by polling machines to obtain data about physical elements comprising the system.

11. (Original) The method of claim 10 wherein the physical elements comprising the system are selected from the group consisting of IP address, machine type, operating system, users, file system structure, vulnerabilities on machines, and programs running on machines.

12. (Original) An apparatus for detecting and characterizing vulnerabilities in a computer system comprising:

a) a processing unit

b) a storage system connected with the processing unit

5 c) an input device connected with the processing unit

d) an output device connected with the processing unit;

e) potential attack set input means for using the input device to load a set of potential attacks into the storage system, wherein the set of potential attacks define attacks through which a change in status of the computer system could be effected, wherein  
10 the change comprises a transition from a start condition to an end condition which is different from the start condition;

f) path set definition means for defining a set of paths comprising at least one path for each attack in the set of potential attacks, wherein each path comprises at least one event necessary for transition from the start condition to the end condition, which

- 15 transition can include passage through intermediate conditions in transit from the start condition to the end condition;
- g) length value assigning means for assigning, for each path in the set of paths, a length value,  $L$ , corresponding to a metric reflecting at least one security significant condition bearing on likelihood of success of an attacker attempting to effect said transition
- 20 from the start condition, through intermediate conditions, if any, to the end condition, so that the value of  $L$  correlates inversely with said likelihood of success;
- h) shortest path identification means for identifying within said set of paths at least one shortest path defined as that having the smallest length value of paths in the set of paths;
- 25 i) epsilon optimal path identification means for identifying, from within the set of paths, specific paths (denoted "epsilon optimal paths") having a length,  $L \leq (1+\epsilon)$  times the length of the shortest path, where  $\epsilon$  is a non-negative number that accounts for uncertainty in individual edge metrics and uncertainty in the actual path the attacker will choose; and
- 30 j) output means for using the output device to communicate "epsilon optimal paths" to a user;
13. (Original) The apparatus of claim 12 wherein the at least one security significant condition is selected from the group consisting of
- 5 estimated time necessary for the attacker to achieve said success,
- estimated cost to the attacker in order to achieve said success,
- estimated degree of effort by the attacker in order to achieve said success,
- estimated likelihood of detection of the attacker's efforts in attempting to achieve said success,
- estimated likelihood of approbation of an attack, and
- any combination thereof.

14. (Original) The apparatus of claim 13 further comprising graphical depiction generating means for generating a graphical depiction of at least a portion of the set of paths, wherein, for each path, nodes represent discrete physical states of the computer system and edges adjoining nodes represent transitions between physical states in the computer system.
15. (Original) The apparatus of claim 14 wherein nodes shown in the graphical depiction include
- a physical state associated with the start condition,
  - a physical state associated with the end condition, and
  - physical states associated with intermediate conditions, if any exist for a given path.
16. (Original) The apparatus of claim 15 wherein redundant paths to nodes are eliminated, by enforcing an ordering on acquisition of multiple, independent vulnerabilities in the graph.
17. (Original) The apparatus of claim 16 wherein transitions between physical states in the computer system are characterized mathematically by assigning each transition an edge weight based on at least one security significant metric having an assigned value.
18. (Original) The apparatus of claim 17 wherein the assigned value of the at least one security significant metric is calculated as a function of an element capable of affecting security of the computer system, wherein the element is selected from the group consisting of
- capabilities of at least one hypothesized attacker and,
  - network configuration information.
19. (Original) The apparatus of claim 18 wherein the capabilities of the at least one hypothesized attacker are assigned a quantitative value based on a factor selected from the group consisting of:
- hypothesized probability of success of the attacker in effecting a given transition between physical states;

hypothesized cost to the attacker in effecting a given transition between physical states;

hypothesized level of effort of the attacker in effecting a given transition between physical states

10 hypothesized length of time necessary for the attacker to succeed in effecting a given transition between physical states; and

any combination thereof.

20. (Original) The apparatus of claim 19 further comprising configuration file input means for using the input device to load at least one configuration file from which is obtained the information about the network and machine configuration of the computer system.

21. (Original) The apparatus of claim 20 further comprising attack template input means for using the input device to load at least one attack template comprising hypothesized attack information which, in turn, comprises at least one attack step which, if successful, could effect a change in status of the computer system given its configuration.

22. (Original) The apparatus of claim 21 further comprising attacker profile input means for using the input device to load at least one attacker profile comprising hypothesized attacker information which, in turn, comprises at least one capability of at least one hypothesized attacker, which, if exercised, could enable said at least one attack step to  
5 take place successfully.

23. (Original) The apparatus of claim 19 wherein the configuration file is generated as a result of gathering information about the network configuration by polling machines to obtain data about physical elements comprising the system.